

About split quaternion algebras over quadratic fields and symbol algebras of degree n

Diana SAVIN

Abstract. In this paper we determine sufficient conditions for a quaternion algebra to split over a quadratic field. In the last section of the paper, we find a class of non-split symbol algebras of degree n (where n is a positive integer, $n \geq 3$) over a p -adic field or over a cyclotomic field.

Key Words: quaternion algebras, symbol algebras; quadratic fields, cyclotomic fields; Kummer fields; p -adic fields

2010 AMS Subject Classification: 11R18, 11R37, 11A41, 11R04, 11R52, 11S15, 11F85.

1. Introduction

Let K be a field with $\text{char} K \neq 2$. Let $K^* = K \setminus \{0\}$, $a, b \in K^*$. The quaternion algebra $H_K(a, b)$ is the K -algebra with K -basis $\{1; e_1; e_2; e_3\}$ satisfying the relations: $e_1^2 = a$, $e_2^2 = b$, $e_3 = e_1 \cdot e_2 = -e_2 \cdot e_1$. Let n be an arbitrary positive integer, $n \geq 3$ and let ξ be a primitive n -th root of unity. Let K be a field with $\text{char} K \neq 2$, $\text{char} K$ does not divide n and $\xi \in K$. Let $a, b \in K^*$ and let A be the algebra over K generated by elements x and y where

$$x^n = a, y^n = b, xy = \xi yx.$$

This algebra is called a *symbol algebra* and it is denoted by $\left(\frac{a, b}{K, \xi}\right)$. For $n = 2$, we obtain the quaternion algebra. Quaternion algebras and symbol algebras are central simple algebras of dimension n^2 over K , non-commutative, but associative algebras (see [Mil; 08]).

In this article we find sufficient conditions for a quaternion algebra to split over a quadratic field. In the paper [Sa; 16] we found a class of division quaternion algebra over the quadratic field $\mathbb{Q}(i)$ ($i^2 = -1$), respectively a class of division symbol algebra over the cyclotomic field $\mathbb{Q}(\xi)$, where ξ is a primitive root of order q (prime) of unity. In the last section of this article we generalize these results for symbol algebras of degree $n \geq 3$, not necessarily prime.

2. Preliminaries

We recall some results of the theory of cyclotomic fields, Kummer fields and p -adic fields, associative algebras, which will be used in our paper.

Let n be an integer, $n \geq 3$ and let K be a field of characteristic prime to n in which $x^n - 1$ splits; and let ξ be a primitive n th root of unity. The following lemma (which can be found in [Ca, Fr; 67]) gives information about certain extension of K .

Lemma 2.1. *If a is a non-zero element of K , there is a well-defined normal extension $K(\sqrt[n]{a})$, the splitting field of $x^n - a$. If α is a root of $x^n = a$, there is a map of the Galois group $G(K(\sqrt[n]{a})/K)$ into K^* given by $\sigma \mapsto \sigma(\alpha)/\alpha$; in particular, if a is of order n in $K^*/(K^*)^n$, the Galois group is cyclic and can be generated by σ with $\sigma(\alpha) = \xi\alpha$. Moreover, the discriminant of $K(\sqrt[n]{a})$ over K divides $n^n \cdot a^{n-1}$; p is unramified if $p \nmid na$.*

Let $A \neq 0$ be a central simple algebra over a field K . We recall that if A is a finite-dimensional algebra, then A is a division algebra if and only if A is without zero divisors ($x \neq 0, y \neq 0 \Rightarrow xy \neq 0$). A is called *split* by K if A is isomorphic with a matrix algebra over K . If $K \subset L$ is a fields extension, we recall that A is called *split* by L if $A \otimes_K L$ is a matrix algebra over L . The Brauer group $(\text{Br}(K), \cdot)$ of K is $\text{Br}(K) = \{[A] \mid A \text{ is a central simple } K\text{-algebra}\}$, where, two classes of central simple algebras are equals $[A] = [B]$ if and only if there are two positive integers r and s such that $A \otimes_K M_r(K) \cong B \otimes_K M_s(K)$. The group operation in $\text{Br}(K)$ is $[\cdot] : \text{Br}(K) \times \text{Br}(K) \rightarrow \text{Br}(K)$, $[A] \cdot [B] = [A \otimes_K B]$, for $(\forall) [A], [B] \in \text{Br}(K)$ (see [Mil; 08], [Ko; 00]). A result due Albert-Brauer-Hasse-Noether says that for any number field K , the following sequence is exact:

$$0 \longrightarrow \text{Br}(K) \longrightarrow \bigoplus_v \text{Br}(K_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Remark 2.1. ([Led; 05]). *Let n be a positive integer, $n \geq 3$ and let ξ be a primitive n -th root of unity. Let K be a field such that $\xi \in K$, $a, b \in K^*$. If n is prime, then the symbol algebra $\left(\frac{a, b}{K, \xi}\right)$ is either split either a division algebra.*

Theorem 2.1. ([Lin; 12]) (Albert-Brauer-Hasse-Noether). *Let H_F be a quaternion algebra over a number field F and let K be a quadratic field extension of F . Then there is an embedding of K into H_F if and only if no prime of F which ramifies in H_F splits in K .*

Proposition 2.1. ([Ki, Vo; 10]). *Let F be a number field and let K be a field containing F . Let H_F be a quaternion algebra over F . Let $H_K = H_F \otimes_F K$ be a quaternion algebra over K . If $[K : F] = 2$, then K splits H_F if and only if there exists an F -embedding $K \hookrightarrow H_F$.*

3. Quaternion algebras which split over quadratic fields

Let p, q be two odd prime integers, $p \neq q$. If a quaternion algebra $H(p, q)$ splits over \mathbb{Q} , of course it splits over each algebraic number fields. It is known that if K is an algebraic number field such that $[K : \mathbb{Q}]$ is odd and $\alpha, \beta \in \mathbb{Q}^*$, then the quaternion algebra $H_K(\alpha, \beta)$ splits if and only if the quaternion algebra $H_{\mathbb{Q}}(\alpha, \beta)$ splits (see [Lam; 04]). But, when $[K : \mathbb{Q}]$ is even there are quaternion algebras $H(\alpha, \beta)$ which does not split over \mathbb{Q} , but its split over K . For example, the quaternion algebra $H(11, 47)$ does not split over \mathbb{Q} , but it splits over the

quadratic field $\mathbb{Q}(i)$ (where $i^2 = -1$).

We want to determine sufficient conditions for a quaternion algebra $H(p, q)$ to split over a quadratic field $K = \mathbb{Q}(\sqrt{d})$. Let \mathcal{O}_K be the ring of integers of K . Since p and q lie in \mathbb{Q} , the problem whether $H_{\mathbb{Q}(\sqrt{d})}(p, q)$ is split reduces to whether $H_{\mathbb{Q}}(p, q)$ splits under scalar extension to $\mathbb{Q}(\sqrt{d})$.

It is known that, for each prime positive integer p , $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ (the isomorphism is $inv_p : Br(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z}$) and for $p = \infty$, $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

We obtain sufficient conditions for a quaternion algebra $H(p, q)$ to split over a quadratic field.

Theorem 3.1. *Let $d \neq 0, 1$ be a free squares integer, $d \not\equiv 1 \pmod{8}$ and let p, q be two prime integers, $q \geq 3$, $p \neq q$. Let \mathcal{O}_K be the ring of integers of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ and Δ_K be the discriminant of K . Then, we have:*

- i) *if $p \geq 3$ and the Legendre symbols $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$, then, the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p, q)$ splits;*
- ii) *if $p = 2$ and the Legendre symbol $\left(\frac{\Delta_K}{q}\right) \neq 1$, then, the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(2, q)$ splits.*

Proof. i) Applying Albert-Brauer-Hasse-Noether theorem, we obtain the following description of the Brauer group of \mathbb{Q} and of the Brauer group of the quadratic field $\mathbb{Q}(\sqrt{d})$.

$$\begin{array}{ccccccc} 0 & \longrightarrow & Br(\mathbb{Q}) & \longrightarrow & \oplus_p Br(\mathbb{Q}_p) \cong (\oplus_p \mathbb{Q}/\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow \oplus_p \varphi_p \oplus 0 & & \\ 0 & \longrightarrow & Br(\mathbb{Q}(\sqrt{d})) & \longrightarrow & \oplus_P Br(\mathbb{Q}(\sqrt{d})_P) \cong (\oplus_P \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \end{array}$$

where φ_p is the multiplication by 2 when there is single $P \in \text{Spec}(\mathcal{O}_K)$ above the ideal $p\mathbb{Z}$ i.e. $p\mathbb{Z}$ is inert in \mathcal{O}_K or $p\mathbb{Z}$ is ramified in \mathcal{O}_K , respectively φ_p is the diagonal map $\mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$ if there are two primes P, P' of \mathcal{O}_K above $p\mathbb{Z}$ i.e. $p\mathbb{Z}$ is totally split in \mathcal{O}_K . Using this description we determine sufficient conditions for a quaternion algebra $H(p, q)$ to split over a quadratic field $K = \mathbb{Q}(\sqrt{d})$.

It is known that $\Delta_K = d$ (if $d \equiv 1 \pmod{4}$) or $\Delta_K = 4d$ (if $d \equiv 2, 3 \pmod{4}$). Since $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$ it results $\left(\frac{d}{p}\right) = -1$ or $\left(\frac{d}{p}\right) = 0$, respectively $\left(\frac{d}{q}\right) = -1$ or $\left(\frac{d}{q}\right) = 0$. Applying the theorem of decomposition of a prime integer p in the ring of integers of a quadratic field (see for example [Ire, Ros; 90], p. 190), it results that p is ramified in \mathcal{O}_K or p is inert in \mathcal{O}_K , respectively q is ramified in \mathcal{O}_K or q is inert in \mathcal{O}_K . So, p and q do not split in K .

Let Δ denote the discriminant of the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p, q)$.

It is known that a prime positive integer p' ramifies in $H_{\mathbb{Q}(\sqrt{d})}(p, q)$ if $p' | 2\Delta$

([Ko], [Ko; 00]). This implies $p' \mid 2pq$.

Since $d \not\equiv 1 \pmod{8}$ and the decomposition of 2 in \mathcal{O}_K (see [Ire, Ros; 90], p. 190), it results that 2 does not split in K .

From the previously proved and applying Theorem 2.1 and Proposition 2.1, it results that the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p, q)$ splits.

ii) Let p' be a prime positive integer which ramifies in $H_{\mathbb{Q}(\sqrt{d})}(2, q)$. In this case the condition $p' \mid 2\Delta$ implies $p' \mid 2q$. With similar reasoning as i) we get that the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(2, q)$ splits.

Remark 3.1. The conditions $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$ from Theorem 3.1 are not necessary for the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(q, p)$ splits. For example, if $d = -1$, the conditions $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$ are equivalent to $p \equiv q \equiv 3 \pmod{4}$. We consider the quaternion algebra $H_{\mathbb{Q}(i)}(5, 29)$, so $p = 5 \equiv 1 \pmod{4}$ and $q = 29 \equiv 1 \pmod{4}$. Doing some calculations in software MAGMA, we obtain that the algebra $H_{\mathbb{Q}(i)}(5, 29)$ splits. Analogous, for $p = 5 \equiv 1 \pmod{4}$ and $q = 19 \equiv 3 \pmod{4}$, we obtain that the algebra $H_{\mathbb{Q}(i)}(5, 19)$ splits. Another example: if $d = 3$, $p = 7$, $q = 47$. We have $\left(\frac{\Delta_K}{p}\right) \neq 1$, but $\left(\frac{\Delta_K}{q}\right) = 1$. However the quaternion algebra $H_{\mathbb{Q}(\sqrt{3})}(7, 47)$ splits. Another remark is that the quaternion algebra $H_{\mathbb{Q}}(7, 47)$ does not split.

We wonder what happens with a quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p, q)$ from Theorem 3.1 when instead of p or q we consider an arbitrary integer α . Immediately we obtain the following result:

Corollary 3.1. *Let $d \neq 0, 1$ be a free squares integer, $d \not\equiv 1 \pmod{8}$ and let α be an integer and p be an odd prime integer. Let \mathcal{O}_K be the ring of integers of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ and Δ_K be the discriminant of K . If the Legendre symbols $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$, for each odd prime divisor q of α then, the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(\alpha, p)$ splits.*

Proof. We want to determine the primes p' which ramifies in $H_{\mathbb{Q}(\sqrt{d})}(\alpha, p)$, i.e the primes p' with the property $p' \mid 2\Delta$. This implies $p' \mid 2\alpha \cdot p$. Since $\left(\frac{\Delta_K}{p}\right) \neq 1$, $\left(\frac{\Delta_K}{q}\right) \neq 1$, for each odd prime divisor q of α , using a reasoning similar with that of Theorem 3.1, we get that such primes does not exist, so the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(\alpha, p)$ splits.

4. Symbol algebras of degree n

In the paper [Sa; 16] we found a class of division quaternion algebras over the quadratic field $\mathbb{Q}(i)$ ([Sa; 16], Th. 3.1) and a class of division symbol algebras of degree q (where q is an odd prime positive integer) over a p -adic field or over a cyclotomic field ([Sa; 16], Th. 3.2). Here we generalize theorem 3.2 from

[Sa; 16], when A is a symbol algebra over the n -th cyclotomic field, where n is a positive integer, $n \geq 3$.

Theorem 4.1. *Let n be a positive integer, $n \geq 3$, p be a prime positive integer such that $p \equiv 1 \pmod{n}$, ξ be a primitive root of order n of unity and let $K = \mathbb{Q}(\xi)$ be the n th cyclotomic field. Then there is an integer α not divisible by p , α is not a l power residue modulo p , for $(\forall) l \in \mathbb{N}$, $l|n$ and for every such an α , we have:*

- i) if A is the symbol algebra $A = \left(\frac{\alpha, p}{K, \xi} \right)$, then $A \otimes_K \mathbb{Q}_p$ is a non-split algebra over \mathbb{Q}_p ;
- ii) the symbol algebra A is a non-split algebra over K .

Proof. i) Let be the homomorphism $f : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$, $f(x) = x^n$. Since $p \equiv 1 \pmod{n}$, it results $\text{Ker}(f) = \{x \in \mathbb{F}_p^* | x^n \equiv 1 \pmod{p}\}$ is non-trivial, so f is not injective. So, f is not surjective. It results that there exists $\bar{\alpha}$ (in \mathbb{F}_p^*) which does not belongs to $(\mathbb{F}_p^*)^n$. Let β be an n th root of α (modulo p). Since α is not a l power residue modulo p , for $(\forall) l \in \mathbb{N}$, $l|n$, it results that the extension of fields $\mathbb{F}_p(\bar{\beta})/\mathbb{F}_p$ is a cyclic extension of degree n . Applying a consequence of Hensel's lemma (see for example [Al, Go; 99]) and the fact that $p \equiv 1 \pmod{n}$, it results that \mathbb{Q}_p contains the n -th roots of the unity, therefore $\mathbb{Q}(\xi) \subset \mathbb{Q}_p$. Let the symbol algebra $A \otimes_K \mathbb{Q}_p = \left(\frac{\alpha, p}{\mathbb{Q}_p, \xi} \right)$. Applying Lemma 2.1, it results that the extension $\mathbb{Q}_p(\sqrt[n]{\alpha})/\mathbb{Q}_p$ is a cyclic unramified extension of degree n , therefore a norm of an element from this extension can be a positive power of p , but cannot be p . According to a criterion for splitting of the symbol algebras (see Corollary 4.7.7, p. 112 from [Gi, Sz; 06]), it results that $\left(\frac{\alpha, p}{\mathbb{Q}_p, \xi} \right)$ is a non-split algebra.

ii) Applying i) and the fact that $K \subset \mathbb{Q}_p$, it results that A is a non-split algebra.

Remark 4.1. Although Theorem 4.1 is the generalization of Theorem 3.2 from [Sa; 16] for symbol algebras of degree n , there are some differences between these two theorems, namely:

- One of the conditions of the hypothesis of Theorem 3.2 from [Sa; 16] is: α is not a q power residue modulo p . With a similar condition in the hypothesis of Theorem 4.1, namely: α is not a n power residue modulo p , Theorem 4.1 does not work. We give an example in this regard: let $p = 7$, $n = 6$, $\alpha = 2$. 2 is not a 6 power residue modulo 7, but 2 is a quadratic residue modulo 7. Let β be an 6th root of α (modulo 7). We obtain that the polynomial $Y^6 - \bar{2}$ is not irreducible in $\mathbb{F}_7[Y]$. We have $Y^6 - \bar{2} = (Y^3 - \bar{3}) \cdot (Y^3 + \bar{3})$ (in $\mathbb{F}_7[Y]$). So, the extension of fields $\mathbb{F}_7 \subset \mathbb{F}_7(\bar{\beta})$ has not the degree $n = 6$. For this reason, in the hypothesis of Theorem 4.1 we put the condition: α is not a l power residue modulo p , for $(\forall) l \in \mathbb{N}$, $l|n$;

- In Theorem 3.2 from [Sa; 16] we proved that $A \otimes_K \mathbb{Q}_p$ is a non-split symbol algebra over \mathbb{Q}_p (respectively A is a non-split symbol algebra over K) and applying Remark 2.1. this is equivalent to A is a division symbol algebra over \mathbb{Q}_p (respectively A is a division symbol algebra over K). But, Remark 2.1 holds iff n is prime. For this reason, the conclusion of Theorem 4.1 is: A is a non-split symbol algebra over \mathbb{Q}_p (respectively A is a non-split symbol algebra over K).

Conclusions. In the last section of the paper, we found a class of non-split symbol algebras of degree n (where n is a positive integer, $n \geq 3$) over a p -adic field, respectively over a cyclotomic field. In a further research we intend to improve Theorem 4.1 from this paper, for to find a class of division symbol algebras of degree n (where $n \in \mathbb{N}^*$, $n \geq 3$) over a cyclotomic field.

References

- [Al, Go; 99] V. Alexandru, N.M. Gosoniu, *Elements of Number Theory* (in Romanian), Ed. Bucharest University, 1999.
- [Ca, Fr; 67] J. W. S. Cassels, A. Fröhlich (editors), *Algebraic Number Theory (Proceedings of an instructional conference organized by the London Mathematical Society)*, Academic Press, 1967.
- [Gi, Sz; 06] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.
- [Ire, Ros; 90] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1990.
- [Ki, Vo; 10] M. Kirschmer, J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714-1747.
- [Ko] D. Kohel, *Quaternion algebras*, echidna.maths.usyd.edu.au/kohel/alg/doc/AlgQuat.pdf
- [Ko; 00] D. Kohel, *Hecke module structure of quaternions*, Proceedings of Class Field Theory - Centenary and Prospect (Tokyo, 1998), K. Miyake, ed., Advanced Studies in Pure Mathematics, **30**, 177-196, 2000.
- [Lam; 04] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, American Mathematical Society, 2004.
- [Led; 05] A. Ledet, *Brauer Type Embedding Problems*, American Mathematical Society, 2005.
- [Lin; 12] B. Linowitz, *Selectivity in quaternion algebras*, Journal of Number Theory **132** (2012), pp. 1425-1437.
- [Mil; 08] J.S. Milne, *Class Field Theory*, <http://www.math.lsa.umich.edu/jmilne>.
- [Sa; 16] D. Savin, *About division quaternion algebras and division symbol algebras*, Carpathian Journal of Mathematics, **32(2)** (2016), p. 233-240.
- [Vo; 10] J. Voight, *The Arithmetic of Quaternion Algebras*. Available on the author's website: <http://www.math.dartmouth.edu/jvoight/crmquat/book/quaternion-modforms-041310.pdf>, 2010.

Diana SAVIN,
 Faculty of Mathematics and Computer Science, Ovidius University,
 Constanta 900527, Bd. Mamaia no.124, România
 Email: savin.diana@univ-ovidius.ro; dianet72@yahoo.com